CYBER SECURITY

Alliott NZ Spring 2019 Newsletter

Alliott NZ Ltd Chartered Accountants & Business Advisers

Message from Greg and Vanessa

Cybersecurity is one of the biggest sources of financial vulnerability to any contemporary organisation. Every cyber breach costs money, but a recent report reveals chief financial officers (CFOs) are currently way down the executive pecking order in terms of who sets the direction for cyber strategy.

Instead, it means that CFOs must work closely with technology experts without abdicating responsibility for risk management. That doesn't mean we have to become tech experts. But we do need to show leadership on cybersecurity spending and governance decisions related to it. In this issue, we look at a few key areas in which you can work to shore up risk. You can also browse our blog for all the articles we've published recently around cybersecurity.

NZ businesses lucrative targets for cybercriminals

Main sources for attacks from email or phishing scams (70%) and hacking attempts (47%).

Businesses that experienced a cyber attack were most likely to have been attacked within the last two years, with almost half (48%) having experienced an attack within the last 12 months.

The main impact of cyber attacks on businesses were:

- downtime (45%)
- inconvenience (41%)
- expense for re-doing work (29%)
- privacy breach (16%)
- financial loss (15%)
- data loss (12%)

Of those that had lost data in an attack, one-quarter of that data (24%) had not been recovered.

"Small businesses dominate the New Zealand economy: 97 percent of enterprises have fewer than 20 employees and 70 percent are sole traders," says Mark Gorrie, Director, Norton Business Unit, Pacific region, Symantec. "Collectively they employ 29 percent of New Zealand private sector workforce and account for more than a quarter of New Zealand gross domestic product. That's a lot of employees and critical business information to protect from cyber criminals."

Almost a third (31%) of business operators surveyed do not believe they would last a week without critical business information.

Despite this, one in five small businesses (19%) back up their business data no more than once a month.

Meanwhile 12% are required to retrieve lost data such as emails or deleted files on at least a monthly basis. Most business operators (62%) are using external hard drives for their backups, while almost one-third were using a cloud provider for their backups.

Alarmingly, 16% of respondents backed up to their own computer and of these, 70% did not back up anywhere else, leaving themselves vulnerable to complete loss of data.

"It is concerning that New Zealand small businesses are leaving themselves and their critical business information exposed and vulnerable," said Gorrie. "When 31 percent of businesses don't think they can last a week without their critical business information – it makes absolutely no sense not to do everything you can to protect it."

BusinessNZ Chief Executive, Kirk Hope, said data protection was necessary for all businesses.

The survey found that 18% of SMBs in New Zealand do not have an internet security solution. The main reason business operators gave for forgoing internet security was that it was not a priority for their business (31%).

Even those businesses with internet security are taking some risks with their critical business information. While 92% of PCs and 89% of laptops are secured, that percentage drops to 61% for tablets and 42% for mobile phones.

“Once infected, nothing matters to cyber criminals but payment – they don’t care about disruption to business or the impact on customers. Not having basic internet security in place will, given time, compromise the business. It’s time for New Zealand SMBs to make online security a business priority and even consider cyber insurance to protect them should they be impacted by a cyber attack,” said Gorrie.

Ransomware prevents or limits users from accessing their system unless a ransom is paid. Only five percent of New Zealand business operators had been affected by a ransomware attack. Of the businesses surveyed who had experienced a ransomware attack, only 13% had paid the ransom, which, on average, had amounted to $1,340. Ransoms were all in US dollars. All businesses affected by a ransomware attack had received their files back after they had paid.

Two-thirds of business operators said they would likely report a ransomware attack to the police. When asked if they would pay the ransom, 68% of business operators didn’t think they would.

“Often people don’t know what to do, don’t understand their options, and don’t have the right security in place to combat a ransomware attack – so they pay the ransom,” said Gorrie.

"Unfortunately, when local businesses pay up it fuels the proliferation of this style of attack. What people actually do when their critical business information is held to ransom is often different from what they think they'd do in that situation."

Source *www.geekzone.co.nz*

Cybersecurity and whaling

Watch out for whalers

One step up from phishing attacks are whaling attempts (aimed at bigger 'fish') where a quite convincing-looking and well-timed email is received by the finance team, purporting to be from the CEO who is perhaps overseas, and asking for a significant amount of money to be transferred to a bank account with the bank details in the email.

Finance teams should be educated about whaling, and processes implemented so that a phone call is made to the CEO to confirm the instruction, or the CEO uses a pre-arranged 'safe' word in the email to authenticate the request.

Organisational checklist

1. Training for employees is vital to ensure they understand the criticality of data and how it, and they, may be targeted.
2. Find, classify and protect your organisation's sensitive data.
3. Deploy software updating/security patches as soon as possible after their release to reduce vulnerability.
4. Employ data encryption to protect sensitive data in transit and at rest.
5. Use firewalls, anti-malware and intrusion detection to protect your environment.
6. Use identity management to control user activity.
7. Understand where your organisation's data is stored and by whom. What level of resilience and recovery plans are in place over these data stores?
8. Evaluate and control risks in the supply chain.
9. Monitor and control devices connected to the corporate network, especially smart devices.
10. Create, regularly update and test both recovery and resilience plans, enabling you to manage a significant attack.
11. Ensure compliance with the data privacy (personally identifiable information) regulations for the jurisdictions in which your business operates.
12. Understand the parties to which the organisation should report cyber intrusions.
13. Consider buying cyber insurance.
14. Consider implementing 2-factor authentication to access all devices in your organisation.

Personal checklist

- Do not click on emails from unknown senders; always verify the address.
- Use malware-blocking software.
- Always update your system and applications with the latest software updating/security patches.
- Use public wi-fi with caution as it may be more vulnerable than private/office systems.
- Vary passwords between websites or services to prevent a compromised account opening up access to others.
- Use credit monitoring services to deal with suspicious activity.

Source: Cyber and the CFO. Article first published by Acuity.partica.online. (2019)

Cyber policies should cover these points

The threat cannot be overstated

1. **Acceptable use:** What company equipment can and cannot be used for.
2. **Access control:** Who can access what, and when and where they can access it.
3. **Change management:** Procedures to ensure that the impact of IT software or hardware changes on security is monitored and communicated.
4. **Information security:** The rules governing the sensitivity of data and the accountability of employees.
5. **Disaster recovery:** How business continuity will be maintained in the event of a successful attack.
6. **Passwords:** Rules covering the format and updating of passwords and their reuse.
7. **Incident response:** How the company will respond to an incident and recover from it, and who will take responsibility for remedial actions.
8. **Remote access policy:** How employees will connect to the organisation's systems remotely.
9. **Bring your own device (BYOD):** How employees should use, connect and encrypt personal devices they use for company business.
10. **Email/communication:** Acceptable use of email, social media, blogs and phone.

Key governance questions

1. Does the board understand the organisation's exposure to cyberattacks from both inside and outside the business, and the extent of the digital connections it has with suppliers, customers and the outside world?
2. What are the vulnerabilities of the organisation to cyberattacks and the risks of it occurring?
3. What are the likely business impacts of cyberattacks, including revenue loss, business disruption, crisis management, regulatory and recovery costs?
4. What is the planned response to a cyberattack to deal with technical resolution, business disruption, impact, reputation management and regulatory response, and mitigating knock-on effects outside the business?
5. What capabilities and resources does the organisation have for managing cybersecurity risks and dealing with incidents?
6. How can the organisation collaborate with regulators, law enforcement, suppliers, customers and other stakeholders?
7. How often does the organisation's cybersecurity preparedness undergo review and testing, and who does the testing?
8. Who is responsible for reporting on cybersecurity, both in an incident-based and regular basis?
9. How often should there be board discussion of cybersecurity?

Source: Cyber and the CFO. Article originally published by Acuity.partica.online. (2019)

Leading cyber risks

CFOs need to take a broader view on risks

1. Phishing

Staff either open attachments or click on links in emails that download malicious code, or they are lured into providing passwords and login details.

2. Malware

Rogue software, such as computer viruses, is loaded onto an enterprise system as a result of a phishing attack or by staff accessing compromised websites.

3. Data theft

Unauthorised system access by hackers leads to data breach and theft. Disgruntled personnel may use thumb drives to download files without authority.

4. Shadow IT

Business units buy cloud-based computing services without the oversight of the IT team, so risk creating systems vulnerabilities when they link these systems to core enterprise applications.

5. Distributed Denial of Service

A coordinated attack using botnets (hijacked computers) to access an online service; the flood of bots blocks access to the service for legitimate users.

6. Ransomware

Malware is used to encrypt company data and a ransom is then demanded to access the encryption key. Ransomware is now in decline as many companies have learned to protect themselves with rigorous and regular back-ups.

7. Zero-day exploits

Hackers may seek to exploit software flaws, using them as a way into a company's systems. Regular software patching reduces the risk.

8. Crypto-Jacking

Hackers gain access to poorly protected computing resources and hijack them to mine cryptocurrencies such as Bitcoin. This dramatically slows computing speeds for bona fide processing. If you have a major cybersecurity event that impacts the organisation's records, whether there is a financial penalty or not, there is an impact on the trust of the organisation and on reputation which will ultimately impact the finances.

Always keep up to date, maintain dialogues with your IT providers, be proactive and take charge.

Article originally published by Acuity.partica.online. (2019)

Take a few mins to strengthen security

Stronger security for your Xero account

Why two-step authentication is essential for your business

Large corporations get most of the publicity when it comes to cybercrime and hacking. But cyber criminals are also targeting small businesses. Security industry research shows that over 40% of cyber attacks last year targeted small businesses and this is increasing. That's why Two-Step Authentication is an important security measure you need to take.

Businesses get subjected to a constant barrage of phishing scams and malicious software attempting to steal user account names and passwords. So it's vital that businesses everywhere ensure they have strong security practices to keep their information secure. Security is an issue that everyone needs to take seriously.

Two-Step Authentication (2SA) is available to all Xero customers to provide an additional layer of security for your Xero user accounts. Using two-step authentication significantly reduces the risk of your Xero account becoming compromised if your password gets stolen by phishing or malware.

Many online services offer additional authentication. Whether it's called Two-Factor Authentication (2FA), Multi-Factor Authentication (MFA), or Two-Step Verification (2SV), it all works in much the same way. Furthermore it significantly increases the security of your account. Xero strongly recommends using 2FA/MFA/2SV wherever it's available. This is particularly important in protecting your email and any other account where you may have sensitive, personal or financial information.

How does Two-Step Authentication work?

When you have two-step authentication enabled you need to provide two authentication "factors" to login, plus your Xero username. The first factor is something you know, your password. The second factor is a unique six-digit code that's generated by a separate app on your smartphone. Try something like the Google Authenticator app, Authy or other similar apps.

With two-step authentication enabled, only the Xero user with access to that trusted device will be able to log in. This makes it more difficult for unauthorised people to access your data.

If you don't have your mobile device with you when you need to login to Xero, you can answer the security questions that you set up when you enabled two-step authentication. We recommend that you only use the fallback questions when necessary. Xero advise strongly against using them as a regular alternative to the authenticator app.

Trusted Device Recognition

In addition, Xero's two-step authentication has trusted device recognition. You'll be able to select "Remember me for 30 days" as an optional setting. If you select "Remember me for 30 days" you won't need to perform the second authentication step on that device for 30 days.

Individual users have the option of enabling two-step authentication when they log-in to Xero. From within the Users Settings page, a Subscriber, or a user with Manage Users access, can see which users of their organisation have enabled Two-Step Authentication.

Security is a constantly evolving issue for the tech industry. We strongly encourage all Xero users – and technology users in general – to remain vigilant about the online solutions they use. If you have any questions about this area, please call Alliott's Xero Specialists in Auckland on 09 520 9200.

Protecting Your Assets and Securing Your Future

The dominant lion may lounge around the place...

But when his territory and pride are threatened, he'll stop at nothing to protect them.

And a typical gorilla father will go to battle with other males, who are known to kill baby gorillas as they try to take over the group. Meanwhile, Emperor Penguin dads are super protective over their mates, their young and the nest, possibly because they play an important role in keeping the eggs warm – balancing it between their bellies and the top of their toes!

These animals are all involved in some kind of asset protection ... and it's often a matter of life and death.

No surprise that humans need to take asset protection seriously too and the stakes can be pretty high.

Asset Protection involves keeping your property out of the hands of someone asserting a right against you, perhaps to satisfy a loan or because of litigation. It is sensible to engage in Asset Protection Planning, whereby non-exempt assets (those subject to creditors' claims) are repositioned as exempt assets (those not accessible to creditors).

Let's be clear that there are laws in most territories that protect creditors against the transfer of assets with the intent to hinder, delay, or defraud a creditor. These transfers will likely be deemed fraudulent and may be reversed by a court. So Asset Protection Planning needs to begin early on the basis that life is uncertain, business is uncertain and there is always the chance of claims against assets.

Asset Protection Planning is closely tied up with your Financial Plan which is based on analysis of your sources of income, current and future expenses, how much wealth you plan to accumulate and what you want to leave to your heirs. Part of the plan is to reposition (current and future) assets so they are exempt from creditors.

Your Financial Plan is closely related to your Estate Plan which defines who will manage your assets and take care of your family after you die (or become incapacitated). Certain corporate and trust structures may protect your heirs from claims against the family assets, giving everyone peace of mind.

It's essential to consider this early. And talk to an advisor. Your accountant is well-placed to help you!

Most humans will not have to fight an invader to the death but neglecting to plan can have devastating consequences. Call the team at Alliott NZ in Auckland to review your approach to protecting your business assets on 09 520 9200.

Using Data to Drive Success

The Shifting Landscape of Sales

The science of plate tectonics is how we explain the movement of continents. Yes, continents are moving all the time ... but extremely slowly!

For instance, it is said that the North American and Eurasian tectonic plates are moving away from each other at about 2.5 centimetres per year!

Fortunately, changes in business don't happen so slowly.

One example is in sales. In previous decades, sales was very much the domain of... well... salespeople. You needed the 'gift of the gab', 'people skills' and a 'good dose of self-confidence' to be successful.

This is changing because even the best salespeople increasingly rely on data to drive their sales approach. And data has become more accessible than ever before and easier to analyse. How well are you using sales data in your business? Is it driving your decision-making?

Some examples:

1. What does it cost you to get a lead (a business opportunity)? This can be calculated from your spending on digital marketing, events, networking functions, advertising and so on.
2. How many leads do you generate in a month or a year? You might also 'rate' these leads in terms of their quality or how advanced they are in your sales cycle.
3. How many of these leads do you convert into revenue - your 'sales conversion rate'? Has this changed in the past few months or years?

Sounds pretty simple, right?

But how do these figures vary depending on the product/service you are trying to sell? Maybe your sales conversion rate is higher for some products? Maybe certain salespeople have a higher sales conversion than others? Have you given any thought to your sales lead times? That means how long it takes to close a deal. Shorter is usually better because selling costs money. Again, it may depend on what product you are selling or who is selling it. You don't need to overthink this and you don't need to answer all questions at once. Rome was not built in a day (and continents don't race around the globe at a rate of knots!!) But it is sensible to develop a thesis on how you can improve sales performance and then find the data to support (or improve) your ideas.

We accountants are not known for our strong sales skills but we are great at surfacing relevant data, analysing it and enabling you to implement change in your business. And what could be more important than finding ways to grow revenue?

Why not take a fresh look at sales data in your business? We're here to help. And remember... this is one area of business where we have to act fast and take charge. Waiting for continents to arrive at their destination will not get us the results we need!

Tech trends that will change the way businesses operate

Speed has its costs, however.

Due to their size, small businesses don't have the capital to cushion a poorly-implemented change. For example, the rise of smartphones and linked technology means we can work from anywhere, but also presents security issues. One socially engineered employee could spell the loss of important client information.

Savvy small businesses work in the sweet spot between early adoption and cautious observance. Inasmuch as new technology introduces risk, it also gives your business an opportunity to grow. Get a jump on the future; prepare your company for these seven tech trends that will change the way small businesses operate in 2017.

1. Chatbots, AI, and machine learning

Look for intelligent apps that use machine learning to curate content, data, or products for customers. In the not-so-distant future, retail transactions might take place through a chat model, where the user logs into an instant message app, tells the chatbot what they want, and the AI offers the best fit based on current stock. This technology could also find its way into support channels where AI locates help documents, bypassing support professionals. AI can work in any chat interface, including phone apps, Facebook Messenger, Slack, Hipchat and SMS.

Slack users already interact with the basic AI chatbot, "Slackbot." This bot uses simple programs to get weather, serve you a GIF, remind you of an appointment at a day and time, and even speak to other apps.

2. BYOD and MDM

In mid-2015, International Data Corporation (IDC) forecasted that nearly 75 percent of the workforce will be mobile by 2020. A more mobile workforce means more vulnerable data, especially in workplaces with a bring-your-own-device (BYOD) policy. When your employees check email and sensitive customer information on their personal devices, that data can be exposed to threats.

One stolen phone, laptop, or tablet can put your security at risk. Data segregation or "containerization" solves this problem by putting company-owned or sensitive data in silos on all devices. Even small companies need to defend themselves against hacking and social engineering, so secure connections are critical. Mobile device management (MDM) systems help enforce some of these policies, but we're starting to see more of those systems become native apps. Safari, for instance, lets you bookmark particular URLs that require VPN access. Small businesses in particular can't afford to open themselves to a security risk.

As mobile productivity becomes increasingly plausible, more business units will (and should) adopt information systems with mobile-friendly interfaces or native mobile apps. For example: cloud-based ERP software with an app for tracking time and expenses and viewing real-time data on the go.

3. Remote offices

Most people who haven't experienced it for themselves imagine the remote office as a Silicon Valley hipster trend or a form of staycation where the employee works from bed or the beach. While there is a higher incidence of pyjamas in remote offices, the dull reality is that most remote workers carve an office out of their homes or the local coffee shop with the strongest wifi connection. And they're actually productive. Sure, meetings happen on Google Hangouts or Skype, but technology keeps people in touch.

There's a financial gain behind working remotely: the U.S. alone could stand to save more than $700 billion if those who had jobs suited to remote work could do so. As asynchronous communication through email and chat services becomes ubiquitous, remote workers can batch their tasks and use the long uninterrupted times to get more work done. No celebrations from the sales team or cupcakes to distract you from your work, and the lack of commute saves time, money and oil.

Real estate is expensive, and when your staff gathers virtually, you can save that overhead and expand your talent pool across geographic boundaries.

4. E-commerce

If your store doesn't have an e-commerce site, potential clients will go elsewhere. Some buyers don't purchase anything that can't be delivered, while others are looking for niche products from undiscovered sellers.

Etsy posted growth numbers again in the second quarter of 2016, as companies of all sizes move to the platform. E-commerce sales alone are expected to reach more than $4 trillion by 2020, twice the projection for 2016. Small businesses need to jump on this opportunity and put their products on the web. Now.

5. Connection-as-a-Service

Over the past few decades, the job market has shifted from a focus on manufacturing and production to services. The newest trend, as you may have noticed, is even more nuanced: connection-as-a-service. Think Uber or Amazon. Despite a recent U.K. legal decision, Uber maintains that it connects contract drivers to riders in need. Amazon connects sellers to folks who need important provisions (and weird stuff too), and will even bring you groceries.

Connecting customers to services and products is big business, but small businesses can invest in this trend, too. Lots of small businesses are partnering with connection services to make their products more accessible via the gig economy and the delivery economy.

6. Subscription-based businesses

In the same vein as connection-as-a-service businesses, companies are moving toward subscription-based models. Subscription services + automated payments = win. Also, subscriptions let you budget and make sales projections because clients pay a recurring monthly fee rather than a single flat payment.

Subscriptions are taking over in monthly beauty or shaving boxes, wine delivery, e-learning, healthy snacks, crafting, chore completion, you name it. Subscriptions can be built into nearly any service or industry. Combine the thrill of getting a package in the mail or a completed to-do list with the ease of automatic payments. Everyone wins.

7. Influencer marketing

Billboards and radio spots are a thing of the past, but social media rules our lives. Instead of paying for ad spaces on traditional channels, influencer marketing gives the microphone to key "influencers" who have the ear or eye of large groups of people.

Think the Kardashians and product placement on all of their social channels, but with more clarity, and perhaps a better reputation. Remember, you have to disclose if you pay an influencer to promote your product. That doesn't mean leveraging important clients doesn't pay off. Influencer marketing has the ability to reach niche and untapped markets and is particularly helpful when targeting millennial customers—who, as Katie Elfering of Forbes reminds us, want to "feel informed and involved instead of marketed to."

None of these tech trends are particularly mind-blowing to the informed business owner, but what may be a game-changer in 2017 is the increased rate of change and adoption that we'll see. Technology tends to have a flywheel effect: adoption breeds faster adoption, which breeds even faster adoption. One thing is certain about 2017: technology will move quickly.

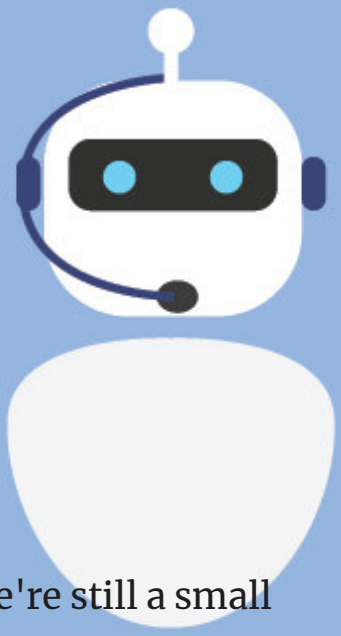
Contact us for a free trial and to speak to one of our Xero certified advisors about how to get the most out of Xero for your business.

Source Xero. Guest post by Tamara Scott, at TechnologyAdvice. Tamara writes about technology, business and SEO.

We've got your Xero data covered with automated backups

As Accountants and Xero Platinum Partners, we recommend that our clients use Xero. Inevitably, our clients also ask what would happen if Xero were to go into outage for an extended period or even ceased operations - how would data and records be accessed. That's the beauty of Control-C. Not only does it provide a daily back up of all your Xero data but it allows offline access to view, search, report and export data as required. As a client of Alliotts, you already receive this as part of our relationship with you.

Connect and leave us a Rating or Review



We work hard to achieve the goals of our clients, but we're still a small business that's very receptive to your ideas and feedback. We'd love to know your views on what it's like to work with the team at Alliotts:

https://www.facebook.com/alliottnz/

g.page/alliottnzcharteredaccountants/review

If you have any questions or queries, please call 09 520 9200 or email enquiries@alliott.co.nz to ask for advice that is relevant to you.

ALLIOTT NZ LTD